UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,690	03/08/2004	Alan Karp	10980964-1	2634

22879 7590 04/28/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
04/28/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/796,690	KARP ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Remarks filed on January 18, 2008.

Claims 1-25 were originally pending.

Claims 1-25 were rejected on July 13, 2007.

Claims 1-25 are currently pending.

Response to Arguments

1. Applicant's arguments filed January 18, 2008 have been fully considered but they are not persuasive.

The Applicant alleges that Mackay does not teach "validating said requesting thread at said local security filter and returning a digital signature that uniquely identifies said requesting thread to said application process." The Applicant continues that Mackay is not validating threads, but the rights of applications to access rights managed content.

The Examiner respectfully disagrees. MacKay teaches "validating said requesting thread at said local security filter and returning a digital signature that uniquely identifies said requesting thread to said application process" [Mediator/shim allows verification and validation of requesting thread through possession of valid certificate. Original certificate is returned to requesting thread. (Col 9, Ln 4-15)]. Mackay is validating threads whether these come from "trusted" applications that have been requesting

access to a protected content. Digital Rights Management is just an example of an embodiment of intended use of Mackay's invention.

The Applicant alleges that Charbonneau does not generate “a first check value associated with said resource request using said validation secret.” Charbonneau fails to illustrate "a security filter comprising a validation secret" and "said system kernel comprising said validation secret." In addition, the Applicant points that there is no indication these applications are in the kernel space, and likely may be in the application space. Furthermore, the Applicant argues that the trusted hash value does not appear to be comprised within a security filter or a system kernel. The arguments presented above are the similar arguments why claims 2, and 20-25 are patentable.

The Examiner respectfully disagrees. As mentioned and cited in the previous action, validating said resource request at said security filter [Secure user-authorization system compares the provided sample with a template retrieved from a user verification database for identity verification.] and generating a first check value associated with said resource request using said validation secret [When verified as secure state, hash values are generated and stored (Page 3 Par 0035).]. In Par 0035, the “predetermined hashing algorithm” including specifications that indicate what data to examine read on the Applicant’s validation secret. Also, Charbonneau discloses “executable code for examining data of the ***operating system*** memory such as the ***DLL tables*** or the ***system call stack***.” This is evidence that executable code or processing involves the

system kernel indicating that the system kernel would have comprised the executable code/instructions to generate the second check value.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claim 1, and 3-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Mackay et al. [US PN 7107448 B1].

Regarding claim 1, MacKay et al. teach a method for safely executing downloaded code on a computer system comprising: accessing an application process wherein said application process makes a system call to a library of said computer system for a resource, establishing a requesting thread [Application to be governed running on a computer system, as such, application process is being accessed. Application makes calls to a modified version of host system's file I/O API, which are handled by a library. (Col 7, Ln 48-50), (Col 8, Ln 16-19)]; sending a request message from said library to a local security filter [A mediator/shim re-implements the actual file I/O calls through a filter. (Col 9, Ln 4-5)]; validating said requesting thread at said local security filter and returning a digital signature that uniquely identifies said requesting thread to said application process [Mediator/shim allows verification and validation of requesting thread through possession of valid certificate. Original certificate is returned to requesting thread. (Col 9, Ln 4-15)]; and making a system call from said application process to a kernel of said computer system wherein said kernel uses said digital signature from said security filter to validate said requesting thread before allowing

access to said resource [Application makes standard call to Governance Engine which inherently resides in Kernel space since it is heavily involved with system I/O calls (Fig 3c, Itm 360). Governance Engine checks credentials (Col 9, Ln 23-26).]

Regarding claim 3, Mackay et al. teach the method as recited in claim 1 wherein said library is a standard ntdll.dll library ["ntdll.dll" library is inherently in Windows platform (Col 8, Ln 66).].

Regarding claim 4, Mackay et al. teaches the method as recited in Claim 1 further comprising: restricting said security filter to an address space that is not accessible by said application [Governance engine may be in the form of a digital rights management application may be installed in a PC as such it is inherent that that there will be program code regarding kernel security residing in kernel space. InterTrust's Inter Rights Point software or Right/System software teaches storing in secure electronic container and/or protected database. (Col 4, Ln 65), (Col 9, Ln 18-19)].

Regarding claim 5, Mackay et al. teach the method as recited in Claim 1 further comprising: said kernel denying access to said resource if said digital signature can not be validated [Col 10, Ln 50-52].

Regarding claim 6, Mackay et al. teach the method as recited in Claim 1 further comprising: downloading executable code initiating said application process [Col 1, Ln

36-42].

Regarding claim 7, Mackay et al. teach the method as recited in Claim 1 further comprising: modifying said kernel such that only system calls that pass through said local library are allowed by said kernel [Presence of governance engine and modified system calls inherently modifies said kernel (Col 8, Ln 38-67).]

Regarding claim 8, Mackay et al. teach the method as recited in Claim 1 further comprising: restricting access of said application process to said resource for one command based on said digital signature [Col 9, Ln 42-43].

Regarding claim 9, Mackay et al. teach the method as recited in Claim 8 further comprising: restricting access of said application process to said resource for one time based on said digital signature ["One time use" is based on "expiring" credentials. (Col 11, Ln 31-34)].

2. Claims 10-14, and 17-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Charbonneau [US Pub No 2003/0074567 A1].

Regarding claim 10, Charbonneau teaches a method for determining the source [whether authorized or unauthorized (abstract)] of a resource request comprising: accessing a resource request associated with an application [Untrusted application

requests for a user data file, instantiates/initiates an action requiring a password (Page 3, Par 0035), thereby, such a resource [data file] request is being "accessed/executed" by the computer system.]; routing said resource request to a security filter, said security filter comprising a validation secret [Password authorization system is a type of security filter and there is a hash generator with a pre-determined hashing algorithm (Page 3, Par 0035).]; validating said resource request at said security filter [Secure user-authorization system compares the provided sample with a template retrieved from a user verification database for identity verification.] and generating a first check value associated with said resource request using said validation secret [When verified as secure state, hash values are generated and stored (Page 3 Par 0035).]; routing said resource request to a system kernel wherein said system kernel comprises said validation secret [Resource request will be further validated and as such, it is inherent that the Kernel is involved.]; generating a second check value associated with said resource request based on said validation secret at said system kernel [Hash generator accesses data stored in one of memory location and using pre-determined hashing algorithm determines a unique hash signature for current state of applications in the computer system. (Page 3, Par 0035)]; and allowing access to said resource if said first check value and said second check value match [Hash verifier performs comparison and fulfills request if verified (Page 3, Par 0035).].

Regarding claim 11, Charbonneau teach the method as recited in Claim 10 further comprising: denying access to said resource if said first check value and said second

check value are different [Page 4, Par 0042].

Regarding claim 12, Charbonneau teach the method as recited in Claim 10 further comprising: storing said first check value in a secure address space that is not accessible to said application [Private key being part of a first check value is stored that is not accessible outside of the trusted group of applications (Page 3, Par 0037).].

Regarding claim 13, Charbonneau teach the method as recited in Claim 12 further comprising: said system kernel retrieving said first check value from said secure address space [Kernel acts upon the hash verifier which includes retrieving keys and hash values for verification (Page 3, Par 0035).].

Regarding claim 14,Charbonneau teach the method as recited in Claim 10 wherein said first check value is a digital signature [A unique hash signature is a digital signature. (Page 3, Par 0035)].

Regarding claim 17, Charbonneau teach the method as recited in Claim 10 further comprising: allowing only resource requests that pass through said security filter to be processed by said system kernel [Resource requests are only allowed when user verification is successful. (Page 3, Par 0035)].

Regarding claim 18, Charbonneau teach the method as recited in Claim 10 further comprising: downloading executable content using said application [Downloading user data file ("content") for usage ("executable" in the context of "executable content" is interpreted as "usable" or "for use") (Page 3, Par 0035).].

Regarding claim 19, Charbonneau teach the method as recited in Claim 10 further comprising: modifying said kernel such that only system calls that pass through said security filter are processed by said kernel [This is inherent because such a security feature taught by Charbonneau in claim 10 involving security application code would inherently modify OS registries thereby modifying said kernel.].

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 2, 10, 15-16, and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mackay et al. [US PN US PN 7107448 B1], and further in view of Charbonneau [US Pub No. 2003/0074567 A1].

Regarding claim 2, Mackay et al. teach the method as recited in Claim 1. Mackay et al does not teach further comprising: sharing a secret between said security filter and said kernel wherein said secret is used by said security filter to generate said digital

signature and is used by said kernel to validate said digital signature. Charbonneau teaches a method for determining unauthorized application execution comprising: sharing a secret between said security application module [hash generator] and said kernel [Operating System] wherein said secret [pre-determined hashing algorithm] is used by [hash generator] to generate said digital signature and is used by said kernel [via hash verifier] to validate said digital signature [Page 3, Par 0035]. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of determining unauthorized application execution by Charbonneau with Mackay's et al. method for safely executing downloaded code on a computer system because the methods of Charbonneau can be implemented as executable programming objects that can be incorporated within the Mackay's et al. security application modules/programs. The suggestion for combining would have been to add security to Mackay's et al method by being able to determine/detect unauthorized executable programs resident in a computer system, thereby also detecting malicious codes such as viruses and Trojan horse applications. Mackay et al. and Charbonneau are in the same field of endeavor of providing security/protection in computer systems from untrusted application programs. Therefore, it would have been obvious to combine Mackay et al. and Charbonneau to obtain the invention as specified in claim 2.

Regarding claim 10, a resource request is inherent in establishing a resource thread. The combined invention of Mackay et al and Charbonneau teaches the method of claim 10 using the same references and rationale as claim 2.

Regarding claim 15, the combined invention of Mackay et al. and Charbonneau teaches the method as recited in Claim 10 further comprising: restricting access of said application to said resource for a single resource request [US PN 7107448 B1, Col 9, Ln 42-43].

Regarding claim 16, the combined invention of Mackay et al. and Charbonneau teaches the method as recited in Claim 10 further comprising: restricting access of said application to said resource for a single time ["One time use" is based on "expiring" credentials. (US PN 7107448 B1, Col 11, Ln 31-34)].

Claim 20 is rejected because it is the apparatus performing the method of claim 2.

Regarding claim 21, the combined invention of Mackay et al. and Charbonneau teach the system as recited in Claim 20 wherein said application is a web browser [Web browser is inherent in networks connected to the internet (US 7107443 B1, Col 1, Ln 40).].

Claim 22 is rejected because it is the apparatus performing the methods of claims 2 and 3.

Claim 23 is rejected because it is the apparatus performing the methods of claims 2 and 4.

Claim 24 and 25 is rejected because it is the apparatus performing the methods of claims 2 and 7.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner. Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132